The network society as seen by two European underdogs

Andrea Monti
alcei@lcei.it http://www.alcei.it
lawfirm@andreamonti.net http://www.andreamonti.net

Italy: a brief note on the background

Italy's legal and political system doesn't have a sound tradition of understanding technology, science and innovation. This is a country that started recovery from "practically zero" at the end of World War Two. It was still basically an agricultural economy, its (limited) industrial resources were destroyed. As late as 1960 there was still a high rate of illiteracy. Technological development was far behind most of Western Europe.

Of course there were, and there are, leading personalities in the world of science and technology. And there are Italian companies, large and small, with strong technological advancement in their specific fields. But in the world of politics and law, and in a large part of the academic establishment, there never was an osmosis between the development of science and technology and the perception of government, legislation and society. Old-fashioned ideas, dating back to Italy's pre-industrial culture, still influence the thinking of people in government and parliament - as well as schools, the intellectual elite and a large part of the citizenship.

This environment has favored the lobbying pressures by major economic forces that have been able to influence legislation (and, to some extent, public opinion) in favor of their private interests, at the expense of civil rights and freedom of expression.

Intellectual property

One example of this distortion is the legislation protecting intellectual property and copyright. A law was enacted in 1992 (d.lgs. n. 518) following a European Union directive (91/250) that extended to software the same protection as for literary authorship. This law defines the duplication of software "for lucrative purpose" as a *criminal* offense punished with imprisonment from one to three years. It was clear that the European directive - obviously inspired by BSA or BSA-like organisation - was intended to repress the sale of illegal copies of software in Italy, but it was interpreted in such a way as to criminalize even private and non-commercial exchanges. As a result, large numbers of kids, students and parents were brought to criminal court for no greater offense than the use of a game that they had borrowed from a friend - or for using at home a copy of the registered software in their

office. Risking up to eight years imprisonment, because in addition to the simple ownership of a copy of software being considered a crime many Public Prosecutors in Italy also consider that in these cases there is an additional criminal charge for receiving stolen goods. The seriousness of this situation lies not only in the fact that the penalties are more severe but also that, while for a "lesser" crime such as duplication of software (art. 171 bis legge 633-41) law enforcement agencies are not allowed to use certain types of investigation, when a more serious crime is suspected (as in the case of receiving stolen goods) they can use more aggressive techniques, including wiretapping. In other words, the private interests of a few large companies (software houses as well as music and video majors) led to the violation of basic civil rights. As a result there was a nationwide "explosion" of inquiries and prosecutions on duplicated software, following this extreme interpretation of the law, involving thousands of terrified (and often completely innocent) victims who couldn't understand why they were being treated as criminals.

A change came after a decision (now famous in Italian law circles) issued by the Court of Cagliari in November 1996, who decided that duplication is to be considered as done "for a lucrative purpose" (and therefore, according to the law, a criminal offense) when the copies are traded (sold for a price) but not in the case of private use or exchange of software. This interpretation of the law caused a furious reaction of the commercial software lobbies, who went as far as to demand a change in the law. The Justice Committee of Parliament is currently considering a change of the words "for lucrative purpose" to "for profit", thus extending the interpretation of the law and once again making it a criminal offense to be simply using, or having installed on one's computer, an unregistered copy of any software - because "profit" can be understood as saving the price of the registration.

Things could get even worse with additional legislation following another European directive that extends the definition of "intellectual property". Future Italian legislation is likely to inflict heavy punishment even for the simple exchange of technical information about the protection of hardware or software - regardless of *why* that is done. In other words, there will be no difference in Italian law between the exchange of information for the sake of training and improvement of knowledge and the "stealing" of proprietary data for commercial purposes.

In addition to all this, legislators are considering the extension to such cases of the incentives offered to people in the large organized crime organizations who are "rewarded" with reduced sentences and other benefits of they "cooperate" with law enforcement agencies. So people will be encouraged to spy on their neighbors or business acquaintances so that they can be subjected to persecution and seizures.

Computer searches and seizing

The seizure of computers is a widespread tool in inquiries. Since 1994 there has been no interruption in a continuing series of seizures, hitting thousands of individual people, families, companies and organizations.

The first and the most famous was the "Italian crackdown" in 1994 (see Giancarlo Livraghi's introduction to this panel). Hundreds of computers (in many cases also monitors, printers, other peripherals, even mouse mats) were seized in the homes and offices of people that turned out to be totally innocent and involved by mistake in the "witch hunt" against assumed software traders. Thousands of users throughout Italy were deprived of their right to use e-mail because the services they were using were abruptly put out; and their privacy was violated because the content of the seized computers (as well as all sorts of backup and storage) were open to detailed inspection by the authorities and by often carelessly chosen "experts".

Aggressive police action, including seizures, was used also in several inquiries that were not chasing duplicated software. Such as hacking (e.g. the "Ice Trap" case, Rome, 1995), pornography (e.g. "Gift Sex, Rome, 1995 and "Ultimo Impero", Milan, 1998) and libel (e.g. "Isole nella Rete", 1999: a server used by several NGOs and voluntary organizations was seized because a Turkish travel agency was irritated by a single message sustaining the Kurd cause).

In many instances, prompted by media hysteria on alleged dangers to national security or morality or potential harm for minors, computer seizures were approved even by important tribunals such as those in Rome and Milan.

Since 1995 it had been clarified on a European scale that *the legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied*. And in fact some enlightened magistrates in Italy have seized what they needed without removing or damaging computers, by making a copy of the relevant information and encrypting the hard disk so that the suspect could continue to use the computer but not alter the "critical" data. Thus demonstrating that it is perfectly possible to conduct effective inquiries without unnecessarily aggressive and damaging systems such as seizing computers.

Wiretapping

During the 1994 inquiries, and those that followed, there were the first experiments of interception of communication between two modems, applying article 266bis of the Rules of Crimanl Procedure_that enact the "network wiretapping". This norm became part of Rules in 1993 by law 1.547 (known as the "computer crime law") that was inspired by a series of recommendations by the European Union inviting member states to include these kind of actions in their national legislation.

Before this particular law only telephone interception was allowed, only in the case of serious crimes (such as arms or drug traffic or usury) and only with the authorized instruments of the inquiring authorities. New legislation introduces a general and undefined concept of "network wiretapping" that can be used for any suspected crime or violation *using information or network_technologies* and can be carried out by any means including *privately owned equipment*.

This causes several problems. The vague definition of "network wiretapping" de facto creates a practically unlimited and unrestricted right of interception - and can coerce private citizens to turn themselves into spies. The law sets no distinction between "voice" (telephone wiretapping) and "data transmission" so there can be situations (such as "voice via IP") where the rules and limitations on phone wiretapping can be bypassed or ignored. Whenever a computer or data transmission are involved (which of course happens more and more frequently) the citizen's protections against wiretapping are de facto removed. All this in addition to the interception and control opportunities offered by mobile phones, which now in Italy are becoming more numerous than corded. Furthermore, the poorly defined criteria in this new legislation involves private subjects (such as ISPs, but practically anyone) forcing them to act as investigating officers without even being compensated for their services.

Encryption and privacy

Of course the wiretapping and interception problems overlap with the general privacy issues and with the right to use encryption.

The situation in Italy is particularly confused. On the bright side, there have never been any restrictions in Italy on the use of encryption (including "strong" cryptography) online or offline. And two recent provisions appear to prohibit key escrow and key recovery. On the other hand, in the case

of "radio amatori" (CB radio speakers) there are old regulations still in force that make it illegal to use encryption codes and allow only the use of specifically authorized languages. So encryption and privacy devices are allowed in wired transmission but may not be in wireless. In this uncertain legal environment, some control advocates are aggressively clamoring on the doomsday risks of "criminal" or "immoral" use of communication and demanding controls on encryption.

The European Union and other international organizations are moving cautiously. On March 27, 1997 the OECD published its own guidelines on the regulation of encryption, but did not deal specifically with key escrow and stated that the privacy rights of citizens are fundamental and can not be violated; indicating that national states *can* (but not "must") set criteria for electronic signatures and encryption systems used by their citizens. Equally careful attitudes were expressed in the European Ministerial Conference *Global Information Network: realising the potential* in Bonn on July 6-8, 1997. In their final document, that summarized many of the questions debated in the EU in previous years, the role of cryptography was emphasized and the OECD position was reiterated: key escrow is by no means a blessing or a necessity.

So... formally, at least, European Union intentions are in favor of privacy and Italy, as a member of the Union, appears to be inspired by these principles. But there are problems. For instance large "portals" and other internet systems are doing all they can to gain personal data that they can sell or use to "profile" customers for the benefit of advertisers. In 1999 the offers for "free internet" multiplied, with many large ISPs and large companies of different sorts (including some that until a short while ago had no interest in online activity) hurrying to get into the act. Of course there is no such thing as "free" internet, as there is a time charge for connection and the various operators share "interconnection fees". But in addition to that many want to use the personal data of users for commercial purposes. There are several violations of privacy, transparency and fairness in contracts. One of the most blatant was denounced by ALCEI in July, 1999. As a result some of the offending contract clauses were changed, but the privacy authority didn't take any action until January 2000 and the "fair competition" authority has not yet issued a decision. So general "good intentions" aren't good enough; civil rights, freedom and privacy watchdogs need to be on alert against many possible ways to try to bypass or misinterpret the rules; by public authorities, private interests or more or less apparent alliances of both.

Bureaucratic obstacles

Italy is notoriously plagued with inefficiency in public administration, too many laws that are often too complicated to be applied properly and conflicting with each other, and all sorts of unnecessary and cumbersome bureaucratic procedures.

The law on "treatment of personal data" (improperly known as the "privacy law") is so porly conceived that, if applied strictly, it could block almost any form of communication (not only online). It would be very complicated to explain the intricacies of this law, but as an example it prohibits sending data to countries "not offering appropriate guarantees" and as no other country has such a complicated law that could (at least in theory) impede communication with most of the world, including the United States.

But there are several other obstacles standing in the way of internet activities. One of many examples is the poor management of domain registration. Until December 15, 1999 no company or legal entity could register more than one domain (except telecommunication companies registered in a special list with the Ministry of Communication, that could register separate domains for the different services offered). Such ridiculous limitation created a sort of "black market"; many had to resort to friends or other companies to be able to register the domains they needed. When the rule was changed, the Italian registration authority was totally unprepared for the clutter of requests; six weeks

later most domains requested on December 15 are still not processed and assigned. And of course the sudden removal of the restriction caused a rush of speculators trying to register names that they hope to be able to re-sell. That may well cause an additional workload for our already cluttered and overburdened law courts; as well as place a few more stumbling blocks on the road to healthy growth in the new economy and the new network society.

Opensource and compatibility

The Italian government is more and more actively involved with the internet. Repeated public statements indicate that communication technology is the key for improvement of public administration and better service to citizens. Though some government bodies are genuinely trying to turn these "good intentions" into facts, results so far are negligible. The lack of a coherent plan and a shared understanding is obvious in often conflicting strategies and decisions and in poorly conceived solutions.

For instance, a law on "digital signatures" was enacted two years ago. To this day nobody (except the technical team working on it) knows how public key algorithms will be implemented in the hardware and software equipment to certify signatures in public service or government controlled procedures. No opportunity is offered to examine the source code or to understand how the project is being implemented. Citizens and society seem to be expected to accept blindly whatever is being done; an "act of faith" hardly deserved by an administration that doesn't have a good track record in the effective use of information technology.

There is no coordination. Some public service organizations are using opensource software, but most are not. The Ministry of Education makes agreements to distribute proprietary software in schools, forcing the education system to obey the whims and restrictions of the owners of those technologies. Different parts of the administration distribute documents, compulsory forms and other materials with no coordination or compatibility, often using proprietary software of various sorts. By doing so they are wasting large amounts of the taxpayers' money as well as forcing citizens to waste time and money if they want access to so-called "technologically advanced services". Law enforcement and military organizations use operating systems of which they don't understand the logic or the structure and that they have never verified or controlled. Etcetera...

In other European countries there are, at least, some attempts to improve the situation. In France, parliament is working on a law to introduce Linux in schools and there are several other efforts to expand the use of opensource software in public administration. In Germany the government is financing the development of Gnu Privacy Guard, an opensource encryption system directly competitive to (but compatible with) PGP - hoping to be able to offer it as a potential European standard. In Italy some parts of the administration are (spontaneously) using opensource software, but there is no central effort in that direction. Quite to the contrary, government and parliament are actively promoting the use of proprietary and incompatible software of which, in most cases, they don't know the source code. The European Union has often declared its intent to consider information technology and electronic communication as key issues; but it has ignored, so far, the problem of compatibility, transparency and open source – while rushing to protect the interests of proprietary software whenever prompted by the powerful lobbies of its owners. In Italy, it's even worse. Civil rights and freedom advocates (specifically ALCEI), a few universities, programmers' associations, even government-supported social and economic research agencies, have been actively challenging these backward strategies; but so far they haven't been able to obtain a radical change. This is one of the crucial tasks for the months and years to come - in Italy as in all of Europe.